UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,444	02/06/2002	Giovanni M. Della-Libera	13768.1074	9546

47973 7590 06/23/2011

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER	
HOMAYOUNMEHR, FARID	
ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
06/23/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte GIOVANNI M. DELLA-LIBERA, CHRISTOPHER G. KALER, SCOTT A. KONERSMANN, BUTLER W. LAMPSON, PAUL J. LEACH, BRADFORD H. LOVERING, STEVEN E. LUCCO, STEPHEN J. MILLET, RICHARD F. RASHID, and JOHN P. SHEWCHUK

Appeal 2010-009072
Application 10/068,444
Technology Center 2400

Before ROBERT E. NAPPI, KRISTEN L. DROESCH and DAVID M. KOHUT, Administrative Patent Judges.

DROESCH, Administrative Patent Judge.

DECISION ON APPEAL

STATEMENT OF THE CASE

Microsoft Corporation ("Microsoft"), the real party in interest, seeks review under 35 U.S.C. § 134(a) of a Non-Final Rejection of claims 1-21, 33 and 34.[1] We AFFIRM.

BACKGROUND

Microsoft's invention is related to a method of providing security in a distributed computer system. Abs.; Spec. ¶¶ 2, 6.

Claim 1 is representative:

> A distributed security system comprising:
> a security policy written in a security protocol independent security policy language, wherein the security policy is configurable to be simultaneously implemented for a plurality of computer devices within the distributed security system, wherein at least a first computer device within the distributed security system operates on an operating platform that supports at least one security protocol that is different than a security protocol supported by a platform of at least a second computer device among the plurality of computer devices wherein the first and the second computer devices process data in accordance with the security policy of the distributed security system.

The Examiner relies on the following prior art:

Rothermel	US 6,787,827 B1	Jan. 13, 2004
Saulpaugh	US 6,850,979 B1	Feb. 1, 2005

[1] Claims 22-32 are withdrawn.

Claims 1-3, 5-19, 33[2] and 34 are rejected under 35 U.S.C. § 102(b) as anticipated by Rothermel.

Claims 4, 20 and 21 are rejected under 35 U.S.C. § 103(a) as unpatentable over Rothermel and Saulpaugh.

ISSUES

Did the Examiner incorrectly find that Rothermel describes a security policy written in a security protocol independent security language?

Did the Examiner incorrectly find that Rothermel describes a first computer device that operates on an operating platform that supports at least one security protocol that is different than a security protocol supported by a platform of a second computer device?

FINDINGS OF FACT ("FF")

1. Rothermel describes a system which allows a security policy manager device to create a consistent security policy for multiple network security devices (NSDs) by distributing a copy of a security policy template to each of the NSDs and then configuring each copy of the template with NSD-specific information. Col. 4, ll. 32-38; col. 4, l. 65-col. 5, l. 7.

2. Each template defines default network information filtering rules for various common services and protocols and uses defined aliases to represent

[2] Claim 32 is listed in the statement of rejection in the Answer and the Briefs. The substance of the prosecution record indicates that claim 33 was intended in place of claim 32. Final Rejection 1, 13; Ans. 12; App. Br. 4; Reply Br. 2. Accordingly, claim 33 is included and treated with claims 1-3, 5-19 and 34.

various specific devices for a particular NSD. Col. 4, ll. 52-55; col. 10, ll. 27-65; Fig. 3B.

3. Configuring the NSD template copies with NSD-specific information includes replacing the aliases in the template copy on a particular NSD with information about the specific corresponding devices that are protected by the NSD. For example, an alias for an HTTP server can be replaced with the specific network address and name of the actual HTTP server. Col. 5, ll. 7-12; col. 11, ll. 18-45; Fig. 3F.

4. Rothermel describes, referring to Figure 1 below, [numbers from Figure 1 inserted], a Network Security Device Management (NSDM) system [100] that includes a security policy manager device [110] able to communicate with multiple supervisor devices [120], [160] which are each associated with multiple NSDs [130], [140], [161], [162]. Col. 6, ll. 7-15.

Rothermel's Figure 1 is below:

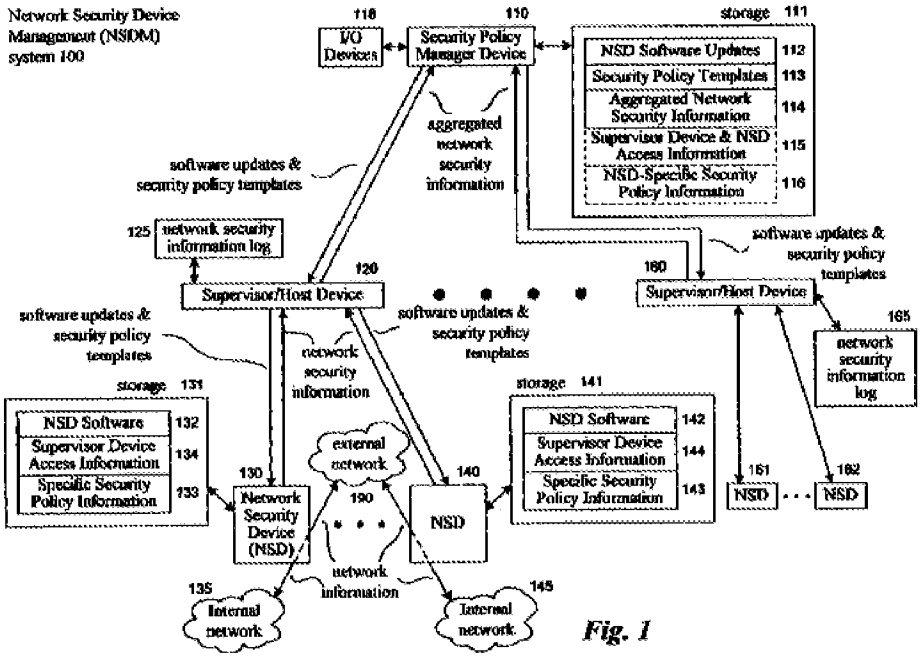

Figure 1 depicts a Network Security Device Management system.

5. Each NSD [130], [140] has a supervisor device [120] designated as a primary supervisor device and stores information about the supervisor device [120] (e.g., device's network address) along with their respective specific security policy information [133], [143], any required access information (e.g., passwords) along with their respective supervisor device access information [134], [144] on storage devices [131], [141]. Col. 6, ll. 33-45.

6. The NSD-specific access information and primary supervisor device information can also optionally be stored by the manager device [110] along with its supervisor device and NSD access information [115] and specific security policy information [116] respectively. Col. 6, ll. 45-49.

7. The security policy manager device [110] stores a variety of information on its storage device [111], including security policy templates [113], aggregated network security information [114] from one or more NSDs, and optionally stores supervisor device and NSD access information [115] (e.g., passwords and a decryption key for stored information) and specific security policy information [116] (including NSD-specific configuration information) for one or more NSDs. Col. 6, ll. 56-65.

8. The security policy manager device [110] has one or more input/output devices [118] (such as a display) to enable a user to interact with the manager device. Col. 6, ll. 54-56.

9. When a user of the security policy manager device [110] desires to establish or modify a security policy for one or more NSDs [130], [140], the user first selects one of the security policy templates [113] or creates a new security policy template. Col. 7, ll. 3-7.

10. The security policy manager device [110] then determines the one or more primary supervisor devices for the NSDs of interest, such as by retrieving this information from its specific security policy information [116]. Col. 7, ll. 8-11.

11. If this information is not stored by the security policy manager device [110], it can be obtained in a variety of ways, such as by querying the NSDs of interest or by querying the various known supervisor devices. Col. 7, ll. 11-15.

12. After the one or more primary supervisor devices are known, the security policy manager device [110] sends a single copy of the security policy template [113] to each of the primary supervisor devices. Col. 7, ll. 16-19.

13. The primary supervisor devices then send a copy of the security policy template to each of the selected NSDs and each NSD stores its copy of the security policy template with the NSD's specific security information. Col. 7, ll. 20-24.

14. Each NSD's copy of the security policy template can then be configured with information specific to the NSD. Col. 7, ll. 25-26.

ANALYSIS

Microsoft first argues that Rothermel teaches distributing a security policy template to network security devices (NSDs) but does not describe, teach or suggest that the security policy template or security policy is written in a security protocol independent security policy language. App. Br. 10-11, citing Rothermel col. 3, ll. 33-34. Microsoft argues that the security policy

template is tailored toward specific devices and must use the existing security protocols utilized by the NSDs. App. Br. 10-11.

Microsoft's arguments are unpersuasive. Contrary to Microsoft's argument that the security policy template is tailored toward specific devices, Rothermel describes distributing copies of a security policy template to a plurality of NSDs and then configuring each copy of the security policy template with NSD-specific information. Col. 4, ll. 32-38; col. 4, l. 65-col. 5, l. 7; col. 7, ll. 16-26; FFs 1, 13, 14. Microsoft also does not direct us to, and we cannot find, where Rothermel describes that the security policy templates must use the existing security protocols utilized by the NSDs. Instead, Rothermel describes that the security policy template defines default network information filtering rules for various common services and protocols and uses defined aliases to represent various specific devices of interest for a particular NSD. Col. 4, ll. 52-55; col. 10, ll. 27-65; Fig. 3B; FF 2. The distributed security policy template copies are configured with NSD-specific information by replacing the aliases in the template copy on a particular NSD with information about the specific corresponding devices that are protected by the NSD. Col. 5, ll. 7-10; col. 11, ll. 18-45; Fig. 3F; FF 3. For example, an alias for an HTTP server can be replaced with the specific network address and name of the actual HTTP server. Col. 5, ll. 10-12; FF 3. Contrary to Microsoft's argument, Rothermel's security policy template is written in a security protocol independent security policy language since it defines default network information filtering rules for various common services and protocols and uses defined aliases to represent various specific devices of interest that are

later replaced with specific information. Col. 4, ll. 52-55; col. 5, ll. 7-12; col. 10, ll. 27-65; col. 11, ll. 18-45;Fig. 3B; 3F; FFs 2-3.

Microsoft further directs attention to following portion of Rothermel's description:

> When a user of the manager device desires to establish or modify a security policy for one or more NSDs such as NSDs 130 and 140, the user first selects one of the security policy templates 113 or creates a new security policy template. Security policy templates are discussed in greater detail below with respect to FIG. 3. The manager device then determines the one or more primary supervisor devices for the NSDs of interest, such as by retrieving this information from its specific security policy information 116. If this information is not stored by the manager device, the manager device can obtain the information in a variety of ways, such as by querying the NSDs of interest or by querying the various known supervisor devices.

App. Br. 11-12, citing col. 7, ll. 3-57 (emphasis in original). In this regard, Microsoft argues that Rothermel does not describe a security protocol independent language because if Rothermel's system could use a security protocol independent security language, there would be no reason to query the specific supervisor devices because any of them could be utilized. App. Br. 11-12.

Microsoft's arguments are unpersuasive because they do not meaningfully explain why Rothermel does not describe a security protocol independent security language based on the need to query specific supervisor devices. According to Rothermel, the need to query the NSDs of interest or the supervisor devices is due to a user (i.e., a system administrator) of the security policy manager device [111] desiring to establish or modify a security policy of one or more NSDs (i.e., NSDs of

interest) and due to the NSD specific security policy information [116] not being stored on the security policy manager device [110]. Col. 6, ll. 7-15, 33-49, 54-65; col. 7, ll. 3-15; Fig. 1; FFs 4-11.

Last, Microsoft argues that Rothermel does not describe or suggest simultaneous implementation across different operating platforms. App. Br. 10-11; Reply Br. 4-6. Microsoft's argument is not commensurate is scope with the claim limitations since independent claims 1, 33 and 34 do not recite different operating platforms. Rather, claims 1, 33 and 34 require a first security protocol supported by an operating platform of a first computer device to be different from a second security protocol supported by an operating platform of a second computer device. We are also unpersuaded by Microsoft's argument that an "operating platform that supports at least one security protocol that is different than a security protocol supported by a platform of at least a second computer device" would inherently have a different operating system. Reply Br. 6 (emphasis in original). Microsoft does not sufficiently explain why a different operating platform would be required to support a different security protocol from the security protocol supported by a second computer platform. It is possible that different security protocols could be supported by identical operating platforms operating on the first and second computer devices.

Microsoft does not separately argue the limitations of dependent claims 2-21. For all these reasons, we sustain the rejections of claims 1-3, 5-19, 33 and 34 as anticipated by Rothermel and the rejection of claims 4, 20, and 21 as obvious over Rothermel and Saulpaugh.

DECISION

We AFFIRM the rejection of claims 1-3, 5-19, 33 and 34 under 35 U.S.C. § 102(b) as anticipated by Rothermel.

We AFFIRM the rejection of claims 4, 20 and 21 under 35 U.S.C. § 103(a) as unpatentable over Rothermel and Saulpaugh.

TIME PERIOD

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

ELD